

www.platon.network

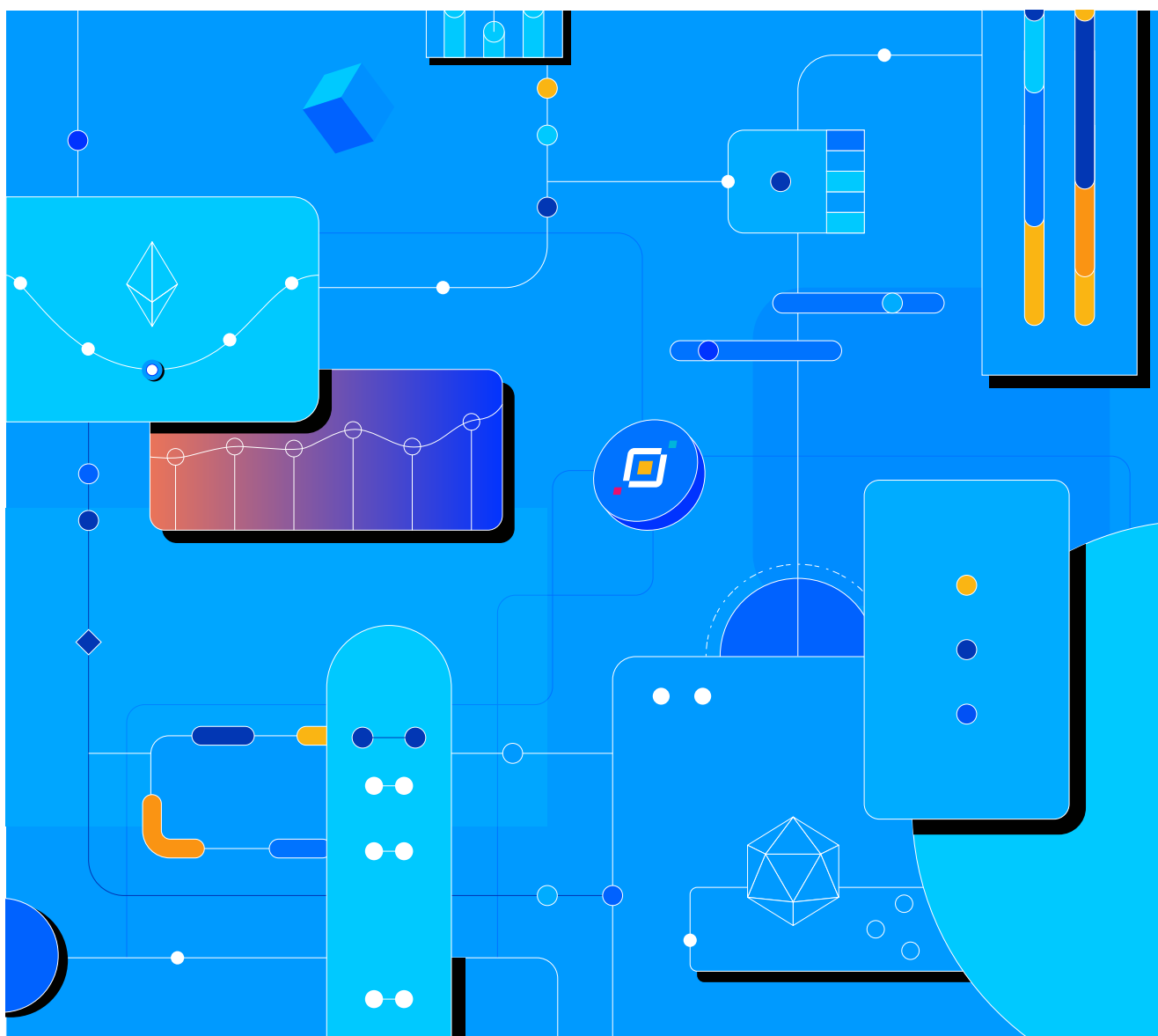


# PlatON

## 应用链技术白皮书

LatticeX Foundation /

—  
2023 | 09 | 22



## 摘要

随着区块链技术逐渐被人们所熟知,越来越多的行业开始关注Web3并致力于在这个领域内寻找发展和构建下一代应用的机遇,然而单一的区块链网络无法完全满足特定行业和应用场景的需求。不同的行业应用各自具有不同的特点和需求,有的需要更高的性能,有的需要更强的隐私保护,有的需要特定的底层技术(如zkp),有的则需要更好的跨链互操作性等等。在公有链无法满足这些特殊需求的情况下,应用链的概念应运而生,旨在为特定行业和应用场景的应用开发提供更加专业化、高效和安全的解决方案。

我们深入研究和分析不同应用的实际需求,提出并制定了应用链整体解决方案的协议,希望通过构建一种通用的、可靠的、标准化的方案,解决特定行业面临的技术挑战和痛点,弥补现阶段区块链基础设施存在的不足,为Web3领域内各行业提供更高效、安全和可信的区块链解决方案,为各行业内的应用在Web3领域内快速落地提供强有力的技术支持,推动数字经济时代的创新和发展。

本文结构如下:第一章介绍了Web3基础设施现状和问题。第二章简要描述应用链在Web3浪潮下的机遇和挑战。我们将在第三章重点介绍基于PlatON构建应用链的整套协议和框架,包括PlatON应用链扩展协议PAEP (PlatON Appchain Extension Protocol),高效的共识机制,可定制化的开发,安全策略以及易用性等方面的内容。第四章介绍了PlatON应用链齐备的基础设施和配套工具集。第五章是实际应用场景的分析。最后在第六章介绍PlatON应用链的生态发展路线规划。



# 目录

<b>第一章 Web3发展趋势</b>	<b>03</b>	<b>第四章 配套的基础设施</b>	<b>22</b>
1.1 多元发展的公链格局	03	4.1 跨链桥	22
1.2 Layer1链的困境	04	4.2 浏览器	26
1.3 应用链的发展趋势	06	4.3 钱包	27
<hr/>		4.4 统一的API服务	28
<b>第二章 应用链的机遇与挑战</b>	<b>08</b>	4.5 隐私计算服务	30
2.1 应用链的定义	08	<hr/>	
2.2 应用链的特征	08	<b>第五章 应用场景和案例研究</b>	<b>32</b>
2.3 应用链的机遇	09	5.1 AI大模型应用链	32
2.4 应用链的挑战	10	5.2 GameFi应用链	33
<hr/>		5.3 DeFi应用链	34
<b>第三章 PlatON应用链</b>	<b>12</b>	5.4 DePIN应用链	35
3.1 基于PoS的应用链扩展协议	13	<hr/>	
3.2 可扩展的应用链框架	17	<b>第六章 应用链的生态系统发展路线图</b>	<b>36</b>

## 第一章/Web3发展趋势

### 1.1. 多元发展的公链格局

不断涌现的新应用和新用户也促进了底层基础设施的快速发展,随着技术的迭代和生态的发展,公有链已经从最初的以太坊“一链独秀”发展到现在的“群雄并起”,这也正是Web3的本质,在去中心化的领域中,公有链这样的基础设施从来都不应该也不可能永久“一家独大”,多元格局之下,崭露头角或正在发展的新兴链亦有在公链赛道继续开拓的空间和潜力。

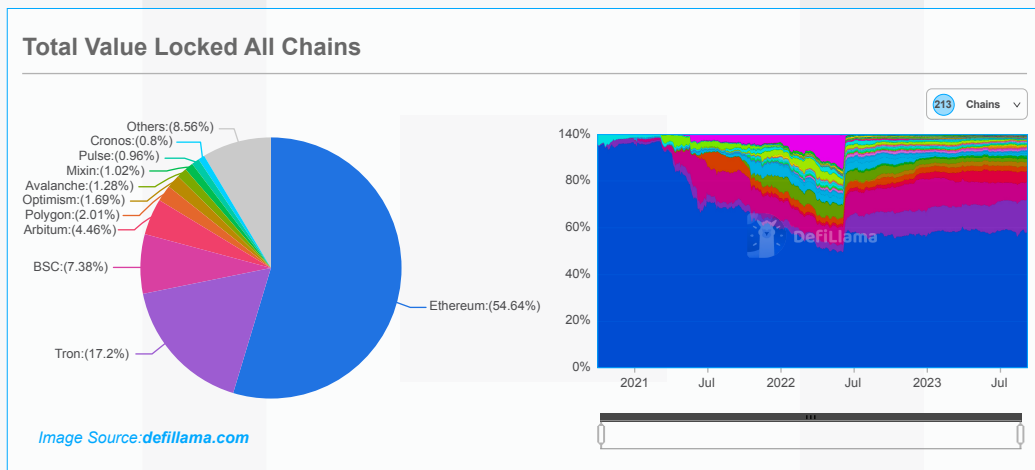


图1 公链TVL数据统计(来自deffilama)

从Deffilama的TVL统计数据可以看出,以太坊依旧占据WEB3生态的主导地位,但是新兴链也呈现出强劲的发展势头,这些新公链可以简单归纳为以下三种类型。

#### EVM兼容链

这类公链的目标很明确,它们不开创新的发展路径,而是在以太坊已有的生态中试图用不同的技术弥补以太坊的不足,例如提升高性能、更快的交易确认时间、更低的能耗等。这类公有链虽然各有各的特点,但由于其选择了跟从以太坊社区,那么可想而知它们想要在影响力上超过以太坊实际上是很难的。

#### 独立开发链

Cosmos和Polkadot从最初就选择从横向扩展链的性能,这样的好处不仅能让链的性能得

到提升,由于子链的相对独立,整个生态链稳定性因不受单点故障的影响而得到保障。而由Meta前员工打造的 Aptos, Sui以及Linera等新公链同样引发一众顶级投资机构关注,这些公链的共同点除了继承了Libra的一些特质外最亮眼的设计就是专门为支付和高频交易设计的并行执行的机制。完全新的架构给新公链提供了各种新的思路,但由于它们都需要各自独立发展生态,短时间内想要达到以太坊的影响力还有很长的路要走。

### 专注某一领域的链

这些链将主要精力集中在解决某领域内的特定问题,谋求在诸如游戏、DeFi、保险等领域内给整个行业带来全新的解决方案,其中代表有dYdX、Immutable X等。这些专有链的发展和现有其他公链可以相互赋能,促进了整个生态的繁荣。

## 1.2 Layer1链的困境

Layer1作为通用的、公共的基础设施不可能是面面俱到和包罗万象的,我们在实际开发的时候,具体到每一种应用的场景,总会有或多或少公有链底层集成更多的能力的期望,然而毕竟有太多人在使用的公链,规则不是谁想改就能改。作为基础设施,Layer1不适合直接承载具体应用。以太坊为例,在其未完全实现分片之前,在以下三个方面无法满足应用需求。

### 高昂的交易手续费

高昂的交易手续费极大的限制了用户和开发者对Layer1的使用,在以太坊网络极度拥堵的情况下,发送一笔普通转账交易的手续费可能高达上百美金,即使是在不算拥堵的情况下发送一笔交易的手续费依然让很多用户望而却步。

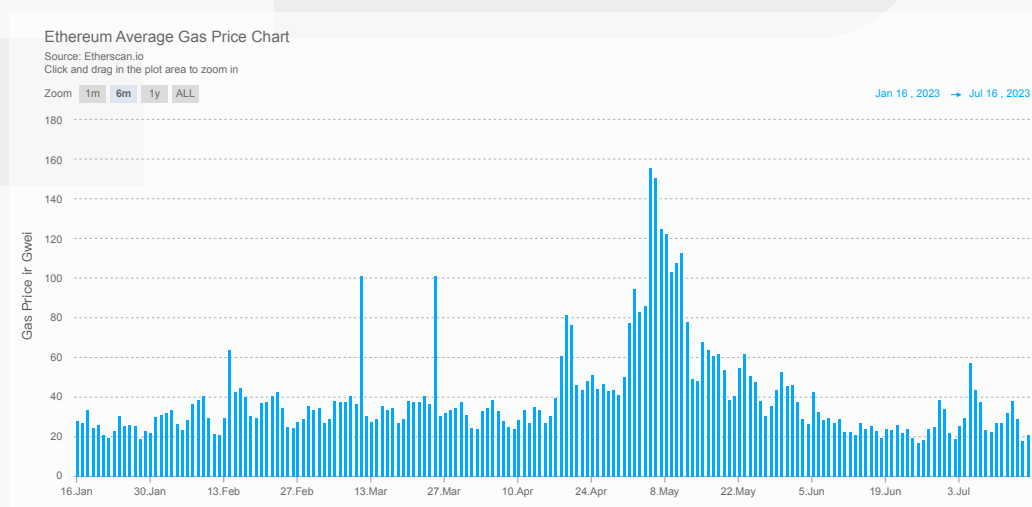


图2 以太坊平均gasprice (来自于etherscan)

## 吞吐量不足

以太坊The Merge合并完成后能耗虽然降低了很多,但每天能处理的交易量依然十分有限,从EtherScan的数据统计可以看出,以太坊每天能够处理的交易量不足120万,平均TPS只有不到14笔/秒。



图3 以太坊日处理交易数 (来自于etherscan)

## 交易确认时间长

低吞吐导致整个网络长期处于拥堵状态,长期的拥堵导致大部分交易不能得到及时的执行和确认,用户体验得不到提升。以下是以太坊网络中最近几天拥堵的交易趋势图。

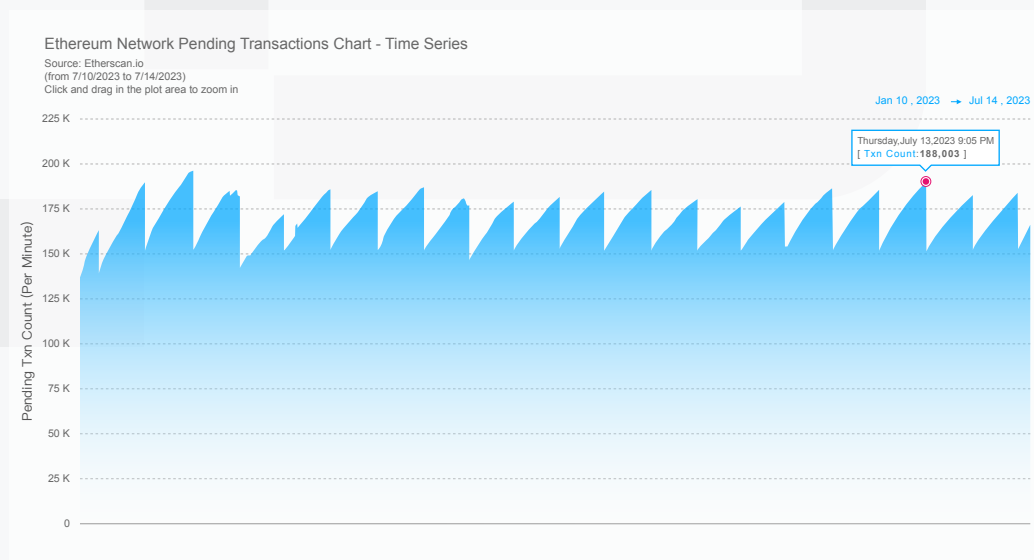


图4 以太坊待处理的交易数 (来自于etherscan)

### 1.3 应用链的发展趋势

区块链技术发展已经到了新阶段,过去十年是基础设施建设阶段,验证了分布式网络、分布式账本、分布式金融三层基础设施的安全性、健壮性、可靠性、可行性。但这三层都是基于DLT和其他WEB3技术的数字新经济的金融基础设施,未来的十年,将要进入到基于这三层金融基础设施之上的、与各种具体的场景、具体的需求、具体的地区相关联的应用开发阶段,区块链技术发展也即将从基础设施建设阶段进入到应用层协议建设阶段。

根据Dappradar 2023.Q2的报告显示,整个二季度每日独立活跃钱包(dUAW)数量较第一季度增长高达7.97%。DeFi领域的TVL继续居高不下,Uniswap协议已经进化到V4版本,GMX更是结合Chainlink的预言机支持动态定价而吸引了一大批用户。NFT市场依旧火热,Blur仍然保持着NFT市场的主导地位,虽然OpenSea和CryptoPunks的交易量出现了短时的下滑,但Immutable X Marketplace和JPG Store却逆势而上,交易量呈现大幅增长令人印象深刻。区块链游戏的用户和应用也稳步提升,占据36%的市场份额。

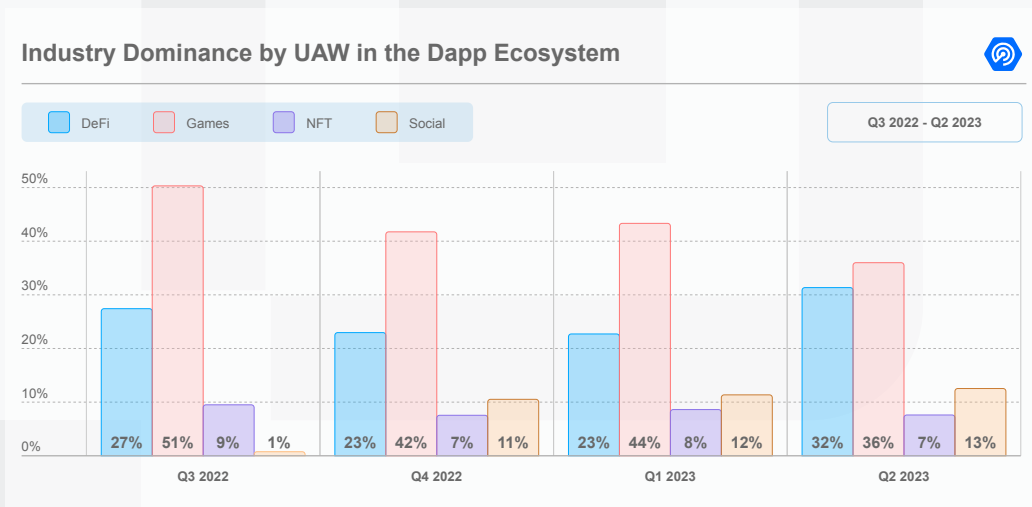


图5 Dapp生态中独立活跃钱包数据统计(来自dappradar)

Layer1既无法做到适配各种应用也不能在性能上无限扩展。以Rollup和Validium为代表的Layer2的基本思想是将公链的功能剥离,将安全性和去中心化机制设计依附在Layer1,将计算和执行下放到Layer2,解决Layer1的交易性能和成本问题。Layer2作为一种扩容方案仍然属于底层的基础设施范畴,并没有从实际支撑具体应用的角度去满足不同的使用场景,仍然有很多应用场景因特殊的需求、区域限制等因素无法直接使用Layer1或Layer2。

在应用协议建设阶段,能支撑这些应用的,不可能直接是Layer1和Layer2,最好的解决方案是基于Layer1的应用链,就像WEB2时代的App store应用分发平台对应用分发起到的作用一样,WEB3时代基于DLT的应用,一定会是应用链模式。





## 第二章/应用链的机遇与挑战

从区块链技术的发展和迭代看，链的分层和角色分工越来越清晰，Layer1明显适合做见证和结算层，Layer2的定位是计算和执行层。应用链的诞生正是源于这种思路，针对特定的应用提供完全独立的链来承载单独的服务，支持特定用例和满足特定需求。

### 2.1 应用链的定义

应用链不同于Layer1或Layer2，也不属于行业链，应用链是针对应用程序定制的区块链，这就意味着应用可以使用链上的所有资源，但和Layer2一样，考虑到安全性，应用链本身并不完全独立运行，它需要依附于已有的Layer1，继承Layer1的安全性。

应用链模式可以说在执行层面将原来的供给驱动改变为需求驱动，将“链”和“应用”的关系细化到了更深入的层次。应用链为开发者提供了灵活性，可微调链的各个方面以满足其应用程序的需求，开发者可以为应用链选择不同的Token Economy、Governance和Consensus等机制。应用链在现有的Layer1之上运行，进一步促进了现有区块链的层级结构和角色的明确分工，为开发人员提供了更多自由。

### 2.2 应用链的特征

应用链在“不可能三角”中偏向满足性能与安全，弱化去中心化。应用链具备如下特征。

#### 专用

应用链的价值在很大程度上体现在专用这个特性上，如果想构建一个需要隐私保护的应用，可以单独开发和部署一条支持多种密码学算法底层的应用链；而想要支持高频并发交易，那也可以开发一条专门支持高频交易的应用链，专用链可以完全不顾及其他不相干的应用。

#### 可定制

现有公链的一个很大的问题就是不能定制化开发，毕竟公有链是大众的基础设施，只能尽

可能满足多数人的通用需求,然而定制化开发却可以让应用开发者专注于特定的业务场景,对于如共识算法、VM、数据可用性服务等其他功能可以直接简单的定制即可使用,极大的提升业务开发速度。

### 可控

应用链是偏中心化或半中心化的平台,这意味着它属于一个特定的应用。而应用的owner应该具有链的控制权,当应用链遭遇黑客攻击或严重故障导致用户受到损失时,应用链的owner应该有一套行之有效的方案,例如冻结资产、回滚区块等保证应用链的安全性。

### 高效

应用链应该支持更高的性能,因其所有资源只属于一个应用,无论从网络规模还是总体账户数都不会太大,因此应用链支持可以支持更高的吞吐量。应用链还可以面向具体应用的业务流程,有针对性地优化以获得更好的性能。

## 2.3 应用链的机遇

应用链的解决方案为整个生态注入了新鲜血液,随着业界对定制化区块链方案的不断探究,已经有越来越多的应用开始意识到开发应用链的必要性。应用链的机遇体现在以下几个方面:

### 多样的生态系统

应用开发的时候经常会遇到兼容性的问题,比如基于Cosmos开发的应用,很难在EVM生态链上部署,EVM上面的应用移植到MoveVM链上也十分困难,应用链作为独立的执行层,可以很好的解决这样的问题,应用开发只需适配一种应用链底层,而无需关注Layer1上是否兼容。

### 高性能执行层

当一些Layer1无法满足应用的吞吐量需求或费用需求时,构建应用链应该是最理想的选择。吞吐量不会受到第三方应用程序活动的影响,因为应用程序配备了专用的区块链,不会与其争夺资源,从而确保了始终如一的流畅体验。区块链游戏应用是最佳示例,大多数互动游戏都需要极高的吞吐量来支持用户的游戏交互,此时部署一个专门为游戏设计的高性能应用链便可以轻松解决性能问题。

### 特定的技术

一些特定的应用需要专门的技术,例如做隐私保护的应用可能要用到零知识证明(zkp)技术,做人工智能的应用会用到AI相关的技术,由于是密集型计算,这些技术无法在Layer1天然的支持,因此使用特定的应用链来支持是比较合适的。

### 经济性需要

对于需要频繁使用底层区块链的应用来说,高昂的交易手续费无疑限制了应用吸引更多用户的能力,而如果使用应用链作为应用的执行层,由于链全部资源只供一个应用使用,没有资源竞争,交易手续费自然会降到很低。

## 2.4 应用链的挑战

应用链一经提出,社区中对其讨论也越发热烈,虽然应用链有以上优点,但对于应用开发者来说现在构建应用链仍然有很多挑战:

### 安全性

应用链继承了主链的安全性,通过Staking和Slashing机制可以让作恶的人付出高昂的代价,但这种机制并不是万无一失的,因为攻击的成本会随着Token的实际价格波动起伏,这就给应用链本身的安全性带来一定的隐患。

### 开发成本

对于一个应用的开发者来说,在Layer1上部署一个智能合约远比开发一条应用链容易的多,应用链的运行会附带一系列需要构建的额外基础设施以及链下的服务。在基础设施方面,需要公共RPC节点来支持钱包和用户与链交互;还需要包括区块浏览器和存档节点在内的数据分析基础设施,来支持用户查看链上信息。除此之外,还有网络监控、跨链、链下Oracle等数据服务。

### 没有通用的协议和框架

对于应用链的开发和部署,现在还没有统一的协议,各公有链上各自制定符合其特点的框架协议,这在很大程度上限制了应用链的发展,与其让应用链开发者适配不同公有链,不如制定一套协议标准,让开发者只需要通过简单的功能定制和接口实现即可轻松完成应用链的开发和部署。

### 缺乏可组合性

应用链是各自独立的,这对于有依赖性的应用来说会增加其开发应用的复杂性。如果是部署智能合约,这种依赖性可以通过跨合约原子操作轻松完成,但在应用链上,开发者不得不考虑从跨链系统获得帮助。

### 跨链带来的问题

应用链和主链交互必须通过跨链系统,资产跨链无疑会增加用户资产风险,而消息跨链的及时性无疑取决于跨链桥的处理性能以及稳定性,都会或多或少的影响用户体验。

## 第三章/PlatON应用链

现有不少以太坊Layer2扩容链提出发展Layer3应用链生态, PlatON作为高性能Layer1基础设施, 不存在可扩展性的问题, 非常适合构建发展Layer3应用链生态。PlatON的技术优势有以下几个方面。

### 性能高

PlatON的架构设计在处理高交易吞吐量和可扩展性方面具有天然优势。PlatON 网络可以支持每秒超过10,000笔交易 (10K+TPS) 的高吞吐量, 以及秒级的交易确认时间 (也称为 TTF time to finality)。这一卓越的性能优势使 PlatON 成为区块链领域可扩展性的引领者。

### 适配性强

PlatON是EVM完全兼容的, 这意味着所有基于solidity合约开发的应用可以直接在PlatON上部署, RPC接口也和以太坊完全兼容, 开发者可以将任何应用稍作调整甚至完全不用做任何修改即可轻松的移植到PlatON上。

### 安全性高

PlatON采用基于权益证明 (PoS) 的共识机制, 该机制经过形式化验证严格证明, 并通过运行时验证 (Runtime Verification), 可确保高度的安全性和可靠性。PoS 机制降低了网络攻击的风险, 增强了生态系统的安全性。

### 基础设施完备

PlatON为开发人员提供丰富的工具和资源, 支持应用链的开发和部署。这使开发人员能够高效地构建应用链。对于开发人员来说, 一个强大的生态系统无疑可以减轻很大一部分开发工作量。PlatON完善的生态系统从钱包、浏览器、SDK、跨链工具、链外Oracle服务、集成RPC服务等多方面为开发者提供支持。

### 手续费低

凭借高性能的基础设施, 交易不存在拥堵问题, 矿工也会尽可能多的打包交易, 这使得 PlatON链上的交易手续费极低。根据 PlatScan 上交易数据统计, 2023年上半年PlatON上的平均交易开销不足0.001LAT, 这无疑将极大的吸引更多的应用开发者在PlatON上构建应用。

PlatON应用链框架方案中,我们基于分层区块链和模块化(Modular- Blockchain)的架构思路,致力于构建以PlatON为RootChain的应用链扩展标准,为各行各业的不同应用场景提供灵活、可靠、一站式的区块链解决方案。

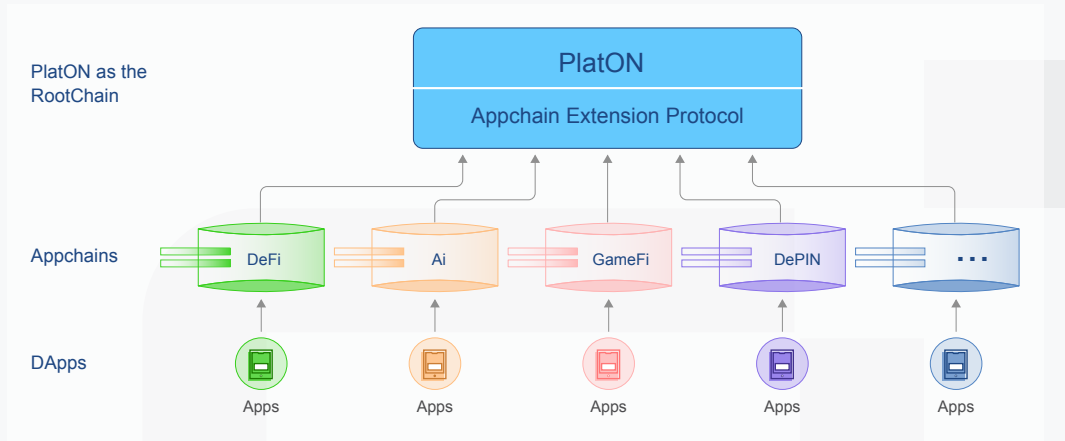


图6 PlatON应用链框架

既然应用链本身不能独立承载应用,那么在应用链和其RootChain之间建立标准的、高效的链间交互协议就变得十分必要,一方面严谨的交互协议可以充分保障应用链的安全性和稳定性,另一方面,通过链间交互的标准化,可以为一众应用链提供标准化的底层接口,适配各种场景,减少不必要和重复的开发。

### 3.1 基于PoS的应用链扩展协议

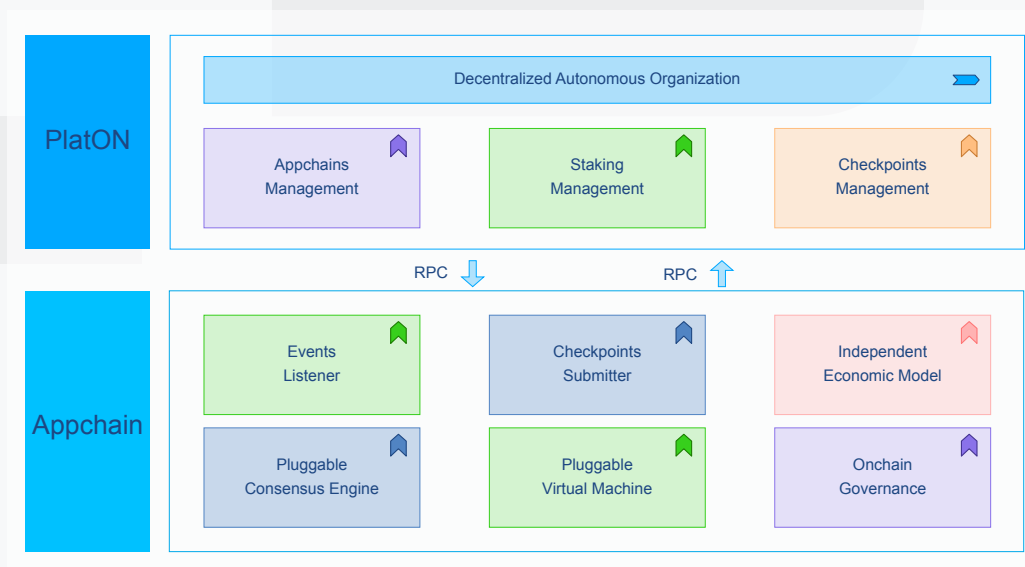


图7 PlatON应用链扩展协议

PlatON的应用链扩展协议将主链 (RootChain) 和应用链 (Appchains) 的角色做了明确的划分,其中PlatON作为应用链依赖的RootChain承担了见证层的角色,而应用链只作为执行层。

### 3.1.1 见证层

应用链本身的设计原则中对“去中心化”特性是弱化处理的,但这并不意味着在应用链上构建的应用就是私有的或者“中心化”的。通过巧妙的设计,我们完全可以使RootChain更多的承载应用“去中心”的属性,成为整个应用链扩展协议的“见证层”。

RootChain作为一个区块链网络的核心,具有较高的安全性和去中心化特性。应用链自身缺少的属性都可以在RootChain上得到很好的弥补。为了让二者有机的结合起来,PlatON应用链扩展协议从以下三个维度规范RootChain在整个框架中承担的职责。

#### 信任

应用链采用高效的共识算法,这类共识算法要求验证节点数量不能太多,但这仅仅是一个可以快速达成共识的普通算法,为了让小范围共识获得更多的认可,PlatON在主网络通过以下方式解决应用链的信任问题:

- 应用链的验证节点必须在PlatON上做Staking, 质押的代币可以是LAT (或应用链的Native Token),也可以是稳定币,一经质押后代币即被锁定。每次参与共识的节点必须从所有质押的验证节点中以可验证的方式随机抽取一个子集, Staking目的—是为了提高成为应用链验证人的门槛,剔除一些质量差的验证人, 另外一方面,通过公开的方式招募验证人并随机抽取参与共识也有保持验证节点去中心化的考量。
- 应用链每隔一段间隔后,要将应用链的状态 (交易树Root、回执树Root等) 结合有效性的证明 (Merkle Proof) 提交到 PlatON作为一个Checkpoint, PlatON将在EVM中对应用链提交上来的 Checkpoint进行合法性验证, 验证通过后将应用链的最新状态登记在Layer1上。

由于应用链验证人的Staking和提交Checkpoint全部发生在PlatON之上, 不仅为应用链验证人设置了准入的条件,也能让应用链的执行结果阶段性的反馈在PlatON上并在主链上对阶段性执行结果进行验证,让应用链的数据更加可信。

## 安全

Staking方案可以提高作恶的门槛, PlatON还结合Layer1上的Slashing来进一步巩固应用链的安全性, 验证节点如果有不作为(例如不出块或不签名)或恶意双出(区块)、双签(Vote)的行为, 一旦被网络中的其他节点鉴别出来, 任何一个验证人即可将证据提交到PlatON上的Staking合约中进行验证, 验证通过后根据协议会对Staking的验证人做出相应的处罚。

## 激励

PlatON的应用链扩展协议是基于权益证明(PoS)的, 为了引入良性的竞争机制, 根据协议规则, 任何维护网络正常运行的节点都将根据质押或委托的周期数、参与共识轮数以及提交Checkpoint等行为受到系统奖励, 奖励的资金来源可以是应用链代币增发、专门的激励池或者是应用链项目方单独设置的基金会。

- **Staking奖励。**质押的节点按质押金额(权重)和质押时长给予的阶段性奖励。
- **委托奖励。**普通账户将代币委托给验证人, 根据验证人设定比例按权重分取的奖励。
- **提交Slashing证明奖励。**为了鼓励节点积极对不作为和作恶的行为进行主动举报, PlatON应用链的Staking合约将按系统参数(参数值可以链上治理)给与举报不作为行为的验证人固定金额的奖励, 而对于恶意的行为, 根据协议会将作恶节点所有的质押金罚没, 并将其中50%奖励给举报的验证人。
- **提交Checkpoints奖励。**Checkpoints作为应用链健康稳定运行的阶段性检查点有着举足轻重的地位, 为了鼓励验证人及时提交Checkpoints, 对于每次提交Checkpoints的验证人节点也将给予固定金额的奖励。

除此之外, PlatON应用链协议还维护了一个可以保证应用链生态健康发展的去中心化自治组织(DAO), 一方面DAO可以积极参与应用链生态的建设, 监督和治理应用链的发展, 另一方面通过这种去中心化治理的方式也可以避免应用链被中心化控制的风险。

### 3.1.2 执行层

应用链作为执行层, 除支持应用开发必要的交易计算和执行外, 还要实时监听主链上和当前应用链相关的事件以及提交本应用链的Checkpoints到主链上:



### 事件监听器

应用链的事件监听器负责实时监听主链上发生的事件,如质押、委托、处罚、奖励领取、验证人退出、应用链系统参数治理更新、版本升级等。一旦监听到本应用链相关的事件将会根据协议由区块提议人发起内部交易,将事件信息同步更新到应用链。

### 检查点提交器

Checkpoint提交器阶段性将应用链上的区块、交易以及回执等信息按照规则(如merkle树)组成固定的数据结构并给出摘要和证明,组成Checkpoint信息,并由轮值的验证节点将Checkpoint发送交易到主链。

### 独立的经济模型

应用链可以独立执行只属于当前应用的交易,也可以有自己独立的经济方案,PlatON应用链内置了一套可配置的经济模型,可以设置有硬顶的总流通量,也可以设置固定的年度增发比例,提议区块可以有固定的矿工奖励,也可以统一在Layer1上进行激励和结算,给应用开发者很大的自由选择。

### 链上自治理

链上自治是通过部署在主链上的DAO等合约,通过发起治理提案的方式完成的对应用链版本升级和系统参数调整的治理机制。

## 3.1.3 应用链治理

应用链按照PlatON应用链扩展协议开发完成后,需要在PlatON主链的AppchainRegistry合约中完成注册,注册成功后可一键部署到PlatON应用链框架,并一键接入到所有基础设施。统一应用链的管理有以下目的。

### 配套基础设施需要

应用链的开发除了执行层意外还依赖很多基础设施,例如浏览器、钱包、跨链系统、支付网关等,统一管理方便在与应用链配套的基础设施中统一注册应用链的ID,方便快捷做好应用链配套组件生成和部署。

### 确保应用链可控

应用链的好处是为开发人员提供更大的自由和控制权,应用的开发者和链上自治组织同时拥有应用链的控制权,这些控制权包括:

- **节点准入**当应用开发者在主链上质押并申请注册一条新的应用链时,其可以选择应用链的节点是否需要准入控制,可以要求节点做好认证 (KYC)、提供特定资质证明或通过白名单 (Whitelist) 的方式控制。
- **2.链上治理**PlatON应用链协议有一套完整的应用链治理框架,应用链自身可选择通过自身治理(当前应用链的验证人作为参与方)和DAO方式治理应用链的提案升级和可治理的系统参数。为了避免资源被恶意占用和无用攻击,注册应用链需先完成质押并成为DAO成员。

## 3.2 可扩展的应用链框架

可定制化开发一直都被认为是应用链最大的立足点,“定制化”对于应用开发者来说可以不仅仅是底层,甚至还包括依赖的其他基础设施。PlatON应用链为开发者提供丰富的组件以便尽可能的为开发者提供支持。

### 3.2.1 可插拔的共识机制

考虑到不同的应用可能对共识算法有不同的需求,PlatON应用链在设计时采用了可插拔式共识引擎设计,提供了引擎接口层,同时实现了built-in的 BFT共识算法和 PoA共识,开发者亦可以通过统一的接口实现自定义的共识机制。

#### 基于Giskard的built-in共识

BFT共识通常需要节点之间广泛的通信和复杂的消息传递,这可能会导致性能问题和高延迟。虽然有一些优化可以改善性能,但与其他共识算法相比,BFT共识可能仍然需要更多的计算和通信资源。

PlatON应用链的BFT共识采用了基于Giskard共识的方案(具体说明可参考PlatON技术文档),并专门针对BFT共识的性能问题进行了优化。通过一系列的技术创新,PlatON应用链有效地提高了共识效率和吞吐量,同时保证了系统的安全性和正确性。

具体来说,PlatON应用链将Giskard共识的流程修改为Leader模式,这样可以将共识消息的广播优化为点对点的消息传输,从而将共识消息数量从指数级优化为常数级。这种优化极大地降低了系统网络资源消耗,提高了共识效率。

在新的出块流程中, Leader提议区块并将其发送给其他验证人, 验证人验证和执行区块, 并将区块投票发送给 Leader, Leader 收集区块投票并发送 QC (Quorum Certificate) 给其他验证人, 最终锁定区块并继续提议区块。虽然 PlatON应用链的 BFT 共识牺牲了一定的去中心化特性, 采用了 Leader 模式, 但同时也保证了系统的安全性和正确性。

### 与Staking结合的PoA共识协议

权威证明 (PoA) 是一种基于许可的共识机制, 通过质押身份来提供快速交易, 并且通过授权的、信誉良好的验证者网络添加区块。然而, PoA共识机制的问题在于过于中心化。

在PlatON应用链中, 为了解决PoA共识机制的中心化问题, 将 Staking机制与 PoA相结合。验证者可以通过质押一定数量的 LAT (或应用链的Native Token) 或稳定币成为验证人, 每一轮出块节点通过VRF (可验证随机函数) 产生随机性选出验证人列表参与出块。

通过这种方式, PlatON应用链既保证了PoA共识的快速交易和授权验证者的信誉良好, 又实现了去中心化的目标。

### 3.2.2 可插拔的虚拟机

PlatON应用链天然支持EVM和WASM虚拟机, 由于底层代码是完全开源的 (基于LGPL开源协议), 通过对底层接口的抽象化, 开发者可基于标准接口做二次开发, 开发出包括MoveVM在内的符合标准的任何虚拟机。

### 3.2.3 可定制的经济模型

PlatON应用链的经济激励机制是可以通过系统参数轻松配置完成, 如代币增发机制、矿工激励策略以及Slashing措施等都可以通过系统参数实现定制, 当然这些系统参数是支持链上治理的。

### 3.2.4 可自定义的链上治理

无论是比特币还是以以太坊, 其区块链底层协议自诞生之日起就在不断演进和自我完善, 受去中心化思想影响, 公有链协议的自我改进的决定权不属于代码的开发者, 也不属于普通用户, 而是属于整个社区。

### 3.2.4.1 链上治理和用途

链上治理通过对治理规则进行编码和存储,结合链上投票和自动计票来决定新协议是否生效的治理方式。链上治理将社区的决策数字化,大大降低了利益相关者的协调成本。传统的链上治理通常做以下用途:

#### 系统参数治理

一些关系到区块链系统安全性和稳定性的核心参数值,很多时候需要根据网络实际运行状况做出适当的调整,例如最大验证人数量、Token年度增发比例以及当验证节点有作恶或不作为行为时扣除质押金的比例等。这些参数的取值受技术迭代、币流通总量和价格等因素影响在不同时期调整到一个大家都认为安全和合理的取值。

#### 重大版本升级

对于不能简单通过调整参数值来修改的底层协议规则,可以由社区发起版本升级提案,同样先在社区讨论论证,经社区表决通过后由开发者完成版本开发和版本交付,验证人升级新版本后发起链上提案和投票,当提案通过后,旧版本因不兼容新的协议而不能再同步主网信息。

### 3.2.4.2 链上治理的问题

传统的链上治理虽然简单和高效,但也有很多不足之处:

#### 缺乏参与

一方面,频繁的治理活动会导致投票人疲劳,不认真履行投票人职责;另一方面,投票人通常对利益不相干提案持冷漠态度,缺乏参与热情。

#### 治理攻击

代币投票系统本质上是财阀控制的,使得那些拥有最高财务利益的人拥有影响决策的巨大能力。这使得治理系统更容易受到贿赂攻击。小额代币持有者无法影响协议改进方向。

#### 激励不足

提案投票要发交易和付交易手续费,然而并没有任何激励投票行为的措施。

### 趋于利益化而非合理化

投票者作为利益相关者通常最在意新协议是否对自己有利,长此以往,改进提案多是趋利性质的而不一定是为了协议的长期成功。

### 缺乏灵活性

大的改进和小的提议都要同样的参与度显然限制了治理的灵活性。

#### 3.2.4.3 可自定义的链上治理

为了解决以上问题,PlatON为应用链精心设计了一套应用链治理合约DAO,将链上治理提案的投票人管理、权重管理和治理方式管理模块化,满足应用链各种治理需求。

### 投票人管理

应用链永远不应该允许验证者获得对治理的控制,因为理性的验证者会不断地试图从应用链经济中获得最大化他们的利益,这直接与其他参与者的利益相冲突,并与加密网络作为最小化利益提取成员 (Minimally Extractive Coordinators) 的理念背道而驰。在项目开始时定义利益相关者及其各种目标对于治理系统的成功至关重要。通过这种方式,您可以解决如何处理任何相互冲突的目标,以便最好地实现平台的总体目标。区块链生态系统中的每个参与者都对生态系统的整体成功感兴趣,因为这是一种互惠互利的运作。治理系统的目标以及“去中心化”治理机制背后的动机是确保针对生态系统做出的决策符合所有参与者的意愿。

所有持有LAT(或应用链的Native Token)的账户都可以通过锁定LAT(或应用链的Native Token)的方式成为DAO成员,DAO成员即是投票人。投票人具有特殊的权力和责任,包括帮助管理链下治理流程(如PIP提案),通过公开透明和数据驱动的意见与社区保持一致,并有权监督和正确的使用选票,还可以直接在链上提议投票,而没有典型的提议门槛。

投票人管理的目的是让专门的人做专门的事,即DAO成员专门负责所有应用链的治理。不同DAO成员对不同的应用链关注和熟悉程度不同,成员要通过积极参与应用链社区讨论和建设获取到利益相关方的支持,以便获得应用链利益相关方的重视,DAO成员从应用链利益相关方(owner、用户、验证人)等获得权益(Token)委托,当权益达到系统阈值后即可参与指定应用链的链上治理。

### 权重管理

围绕治理设计的一个重要且经常被忽视的问题是生态系统利益相关者的权重。对于基于区块链的平台,许多对网络成功至关重要的资源都是参与者自愿贡献的,比如矿工节点的硬件资源。这些关键的资源对整个网络的运行起到至关重要的作用,因此我们在考虑治理的权限分配时要给与足够的考虑。权重管理制定了一套不同性质的Token(如自由流通的Token、验证人锁定的Token)各自权重比例的规则,可以由应用链开发者或运营方自定义和管理。

### 治理方式管理

在设计治理过程时,必须了解需要在治理过程中做出哪些决定。生态系统面临的众多决策可能会受益于不同的治理流程。例如,有些决策需要专有信息,需要专家的参与,而有些决策则需要纳入社区成员的偏好,以便决策获得足够的支持。预先列出随着时间的推移需要升级的操作流程类别,以及所有可能需要做出的决策,将有助于确保建立一个有凝聚力且稳健的治理系统。治理方式管理允许项目自定义治理决策类别。这些类别包括决策需要投票的阶段和轮数,决策划定投票权的规则、投票法定人数、可用投票的数量、如何计算选票和通过率等。

综上,PlatON通过模块化治理框架通过DAO的方式解决了治理疲劳和治理攻击等一系列问题,为开发者提供了更加灵活和可行的链上治理解决方案。

## 第四章/配套的基础设施

应用链单独开发的难度让一些开发者望而却步,为了进一步降低应用链开发的难度,PlatON除制定了应用链扩展协议和应用链框架以外,还提供了丰富的周边配套应用和工具,可支持一键部署应用链,从根本上解决应用链开发难的问题。开发者只需要将主要精力聚集在如何对其开发的应用做好底层支持,无需关心周边设施的开发和部署。

### 4.1 跨链桥

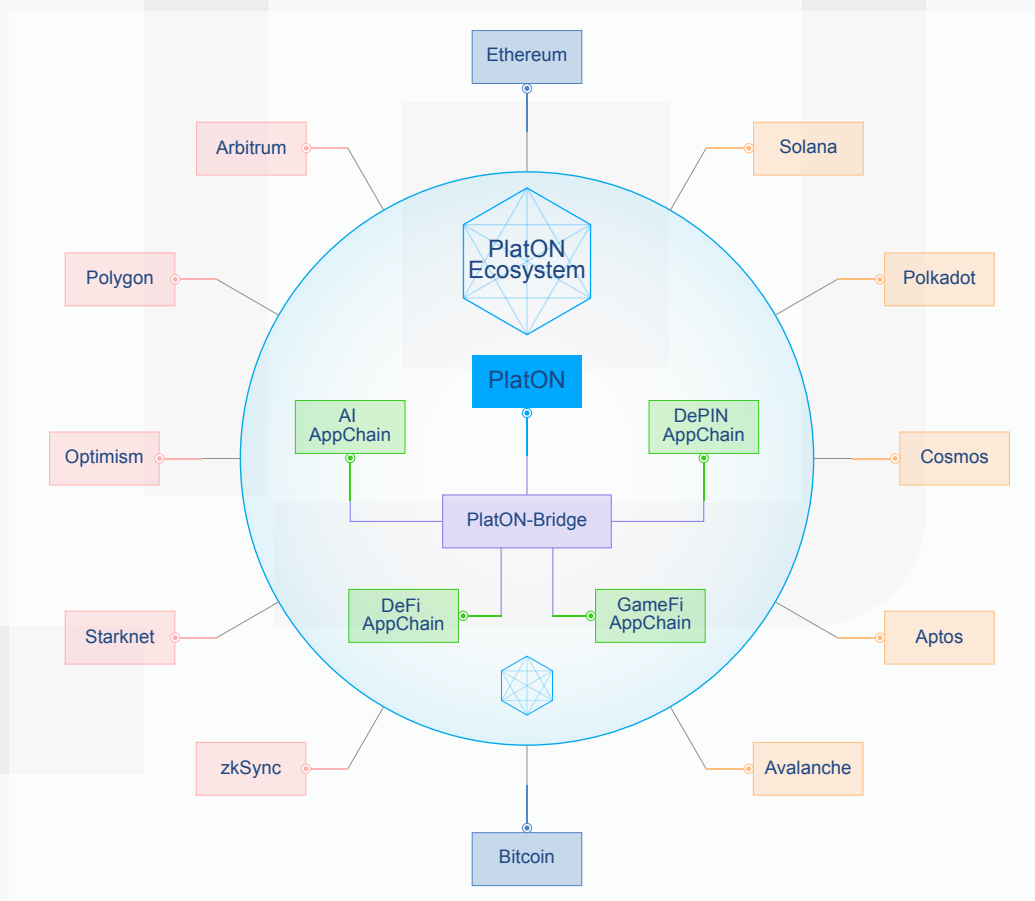


图8 PlatON跨链桥

PlatON-AppChain为开发人员提供了高效平台,以运行对吞吐量、安全性和成本的要求的应用程序。然而,每个独立的AppChain将导致网络碎片化,每个链都是孤立的。所以需要跨



链来组成超级网络。PlatON-Bridge基于消息的流动,消息的传递不受制于合约虚拟机的限制(如 EVM、WASM、Move等)。如图,通过 PlatON-Bridge 跨链桥不仅将 AppChain 网络联通,也将打通 AppChain与PlatON生态以及其它Layer1公链生态。AppChain 的消息流动、资产流动,也将创造出价值生态网络。

PlatON-Bridge 跨链桥作为AppChain网络中一部分,我们选择外部验证的方式进行跨链,也就是PlatON-Bridge跨链桥本身作为AppChain网络中的链。这样的优势是减少其它AppChain的复杂度,AppChain无需监听网络中链的消息,降低AppChain的通信复杂度;足够的去中心化保证,PlatON-Bridge跨链桥本身作为 AppChain,采用BFT共识的方式对跨链消息进行确认,确保不会被恶意篡改。同时为了保证网络的安全性,验证人的数量将会根据PlatON-AppChain的规模进行调整,网络初期,PlatON-AppChain网络中只有少量的AppChain,网络总的价值较小,则验证人数量可以为 25+,网络发展后,全网络总价值不断提升,验证人可以由 25 到 35 再到 45 等,确保跨链网络的去中心。PlatON-Bridge 跨链将成为Appchain网络流动的基础。

PlatON-Bridge 采用 AMB (Arbitrary Message Bridge) 跨链桥的方案,根据项目需求,可以将源链的任意消息类型通过 PlatON-Bridge 传递到目标链。PlatON-Bridge 开发者提供合约套件,合约套件中包含跨链消息的发送,接收等模块,开发者只需要关注业务,将业务合约部署即可完成跨链应用的开发。

PlatON-Bridge 对 EVM 生态进行支持,不仅仅能将 AppChain连接在一起,同时对其它 EVM 的公链(如 Ethereum、BSC、Polygon 等)进行支持,通过部署合约套件,PlatON-Bridge 将不同网络生态与 PlatON 生态进行连接,促进生态发展。基于 PlatON-Bridge 开发者可以构建 DeFi、Oracle、Social、Oracle、Gaming等等不同类型项目。PlatON-Bridge 不仅支持 EVM 生态,对 WASM、Move等合约生态后续也将支持,通过PlatON-Bridge将会构建出全网络的消息流动。

资产的流动是PlatON-AppChain 生态的重要方向,PlatON-Bridge 基于 AMB 跨链桥构建了资产跨链桥,利用 PlatON-Bridge 的AMB跨链消息机制以及完善的跨链合约开发套件,不仅仅能对 PlatON-AppChain 生态的资产进行流动,对 AppChain 与 PlatON 生态以及 AppChain 与其它Layer1生态进行资产的流动转移,通过 PlatON-Bridge 的资产跨链桥,用户的资产流动性增强,也将促使更多应用创新。



#### 4.1.1 跨链架构

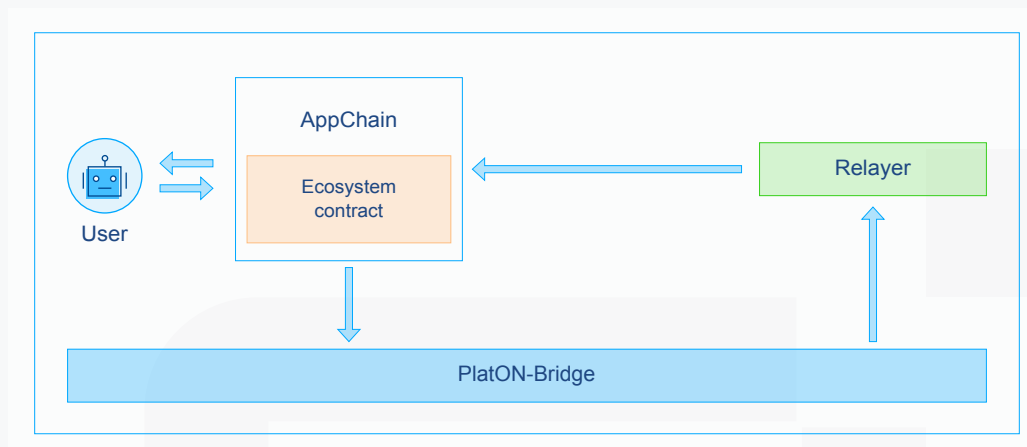


图9 PlatON跨链桥架构

PlatON-Bridge 由 Ecosystem Contracts, Bridge, Relayers 组成。

##### Ecosystem Contracts

生态合约主要是由 PlatON-Bridge 治理的合约,属于 PlatON-Bridge 生态系统内部,主要任务是为其它 AppChain 开发者提供 PlatON-Bridge 功能套件。

##### Bridge

作为一条跨链桥 AppChain,采用PoS + BFT的形式构建,由PoS模型选举出验证人再由BFT对跨链消息进行共识确认。为了保证跨链桥的去中心化,我们计划邀请行业中具有影响力的项目方参与到验证人当中。

与传统的 PoS Chain 验证人只验证链自身的交易不同,跨链桥验证人不仅要验证自身的交易,同时要监听 PlatON-AppChain 网络中其它AppChain的跨链交易信息,每个验证人需要对跨链交易信息进行验证,并将跨链信息转换为跨链桥的 VTA (Verifiable Transaction Approval) 交易。并将 VTA交易打包为区块,由BFT验证人进行验证签名。

##### Relayer

Relayer 在整个跨链流程里发挥着重要作用,如果说 Bridge 扮演着从源链「读取」的角色,那么Relayer则扮演着向目标链「写入」的角色。尽管 Relayer 是 PlatON-Bridge中重要的组成部分,但 Relayer 对安全性不能构成威胁,只对活跃性有影响。也就是 Relayer只负责将 Bridge 的 VTA 信息传递到目标链,不能通过修改VTA 来篡改目标链信息。基于此,Relayer

是目标链交付,那么 Relayer 将可以有多种形态。

- **客户端 Relayer**, 客户端 Relayer 可部署在钱包与浏览器中,有用户客户端负责 Relayer 的交付工作,虽然其简化了开发流程,但是却使用户的操作流程变得极其繁琐,同时用户也必须为 Relayer 支付链上交易费用。所以在一个成熟的项目中并不会选择此种方式,但在一些MPV中,需要快速验证原型的工作中,是一个不错的方案。
- **专用 Relayer**,应用项目方可以通过添加专用 Relayer 来负责指定类型的 VTA交易,从而解决了客户端 Relayer体验问题,专用Relayer也可以通过聚合等批处理手段来减少 VTA交易的 Gas 费用,降低成本。虽然专用 Relayer被称为「专用」,但仍然是不受信任的角色,但提交的 VTA 是公开不可篡改的,所以提交的VTA是被「信任的」。
- **通用 Relayer**, Relayer 作为 PlatON-Bridge 重要组成部分,PlatON官方也会推出通用 Relayer ,来简化用户体验,提升开发人员的效率。

#### 4.1.2 跨链安全性和治理

PlatON-Bridge将由PoS选举出的验证人进行BFT共识,验证人节点将由知名项目方进行背书。为了保证源链的信息可靠性,每个验证人将对各AppChain部署独立的全节点,验证人也会对每笔链上跨链交易生成状态证明,可提供给任一方进行独立验证。

PlatON-Bridge 将通过链上治理的形式进行,我们将在 PlatON 上部署PoS,治理合约,负责验证人的选举及合约升级。目前治理的主要方向包括,修改验证人集合;验证人集合的扩张;生态合约的升级;所有的链上治理合约都将开源,也会邀请多家行业知名审计公司进行审计。

为了保障 Relayer 交易的安全性,我们为 Relayer 提供 MPC 密钥管理服务进行分布式密钥生成以及签名服务。分布式密钥能够确保个人丢失子分片,也不会影响 Relayer 系统安全。此外,我们还可以使用传统身份验证方法,例如双因素身份验证(2FA)来增强该系统的安全性,甚至可以定时或手动刷新子分片。分布式签名也将确保 Relayer 签名不被任意一方操控来发起非法交易,保证签名的安全性。

## 4.2 浏览器

PlatON的应用链浏览器自动支持应用链上区块和交易信息的收集和展示,应用链只需要通过统一注册后获取一个属于应用链的ID,并简单配置应用链的账户地址格式、代币单位以及代币总量等信息即可轻松完成浏览器的部署。

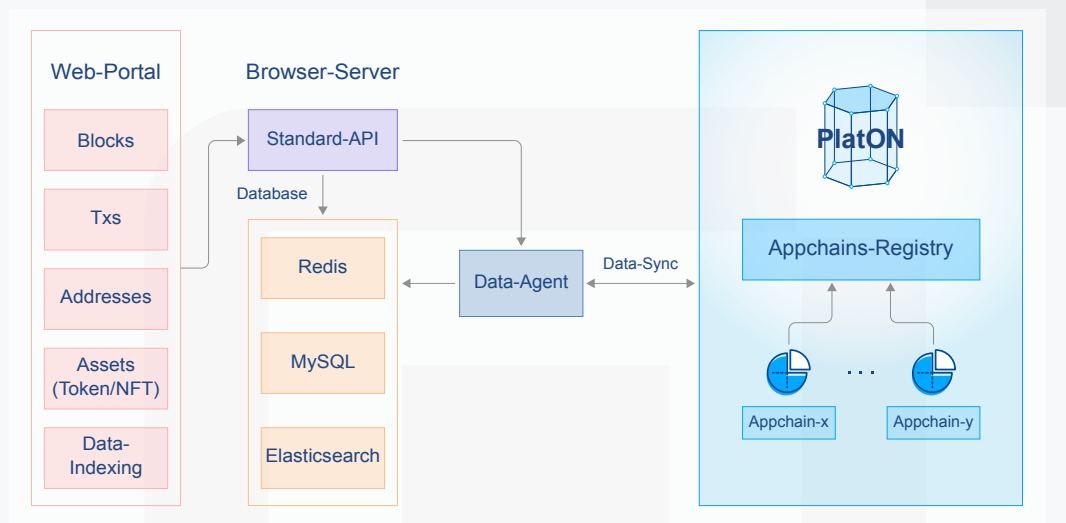


图10 PlatON应用链浏览器架构

### Web-Portal

Web门户提供了模块化功能组件,包括标准化的区块、交易、地址、资产(Token/NFT)等模块,还支持各应用链自定义的数据展示。

### Browser-Server

Browser-Server是统一的应用链浏览器服务端程序,提供标准的数据查询API。

### Database

存储层使用三种不同DB来处理用户不同类型的数据查询需求:

- **Redis**。用于存储常用的热点数据,例如常用的ERC20合约地址、多次重复请求的地址等。
- **MySQL**。MySQL用户存储复杂的关系型数据结构,例如质押->委托关系,治理提案和投票进度等。
- **Elasticsearch**。Elasticsearch用户支持大批量数据查询和遍历,如区块、交易等数据。

### Data-Agent

Data-Agent是一个数据代理服务,用于监听和同步不同应用链的链上数据,一方面可以将链上标准数据如交易、区块等同步写入DB,另一方面也可以实时响应Browser-Server的查询请求直接通过RPC读取应用链的链上数据。

除普通的区块浏览器外,PlatON应用链还有专门NFT定制的浏览器,为NFT应用的开发提供了极大的便利。

## 4.3 钱包

钱包是大多数人进入WEB3世界最先了解和使用的工具,它也是WEB3生态最重要的基础设施之一。发展到现阶段,钱包早已从最初的简单的转账和账户密钥管理功能发展成功能涵盖WEB3领域所有能力的主要工具,随着DeFi、NFT、GameFi等领域内众多项目的实际运营,我们已经看到了传统应用在WEB3实际落地的希望,在这个关键的节点,钱包更是成为了引导用户从WEB2进入WEB3的关键角色。

为了更好的给应用开发者吸引用户提供强有力的支持,PlatON生态中既提供可以直接使用的即用钱包,也有为用户管理密钥和资产提供的钱包服务,同时PlatON还有支持开发者定制开发的钱包插件和SDK。

### 即用钱包

- **ATON:**PlatON的ATON钱包后台服务会自动监听PlatON应用链管理合约,当新的应用链注册成功后ATON后台服务随即按应用链的ID、地址格式和Token名称等信息激活新应用链的钱包服务,应用链开发者无需做任何开发,不用做任何定制即可直接使用ATON上的所有钱包功能。
- **WEB钱包:**随着越来越多的用户习惯于在网页中使用钱包,WEB钱包的发展可谓日新月异。PlatON的应用链浏览器集成PlatON应用链WEB钱包插件,该插件集成了MetaMask、WalletConnect以及Particle等第三方钱包,用户可以选择任意钱包来轻松接入应用链,第三方钱包还支持使用社交账户登录和社交恢复功能,极大改进用户使用WEB钱包的体验。
- **第三方钱包:**PlatON已经接入imToken、Mathwallet、Tokenpocket、Coin98、

Bitkeep、Cobo、Bitpie、Particle、OpenBlock、Unipass等多个第三方钱包,其他支持EVM兼容链的钱包也只需要简单的配置即可直接用于PlatON应用链。

### 钱包的基础服务

- **MPC密钥托管服务:**对于安全性要求极高的重要账户,用普通即用钱包来管理有一些安全隐患,为了降低风险,业界常用的做法是将单点的风险转移到多方进行参与和管理。MPC密钥托管钱包就是典型的解决方案。PlatON的MPC密钥托管服务支持通过安全多方计算的方式生成和管理密钥分片,当前支持ECDSA和BLS两套体系密钥的2-2和2-3算法,其中2-2算法服务支持用户和MPC服务端通过算法协商各自的密钥分片,用户持有一个密钥碎片,MPC服务端管理用户的另外一片碎片,需要转账时需2个参与方共同计算才能对转账交易签名。而2-3算法则支持用户持有两片密钥分片,MPC服务端只保存一片,用户平时使用其中一片用于和服务端分片签名,当用户其中一个分片不小心遗失,用户使用另外一片密钥分片和服务端仍可以完成转账,极大的提高了账户的安全性。
- **抽象账户公共服务:**PlatON支持EIP-4337标准,提供统一的标准Bundler服务,在公共的Paymaster合约中默认使用LAT(或应用链的Native Token)作为发送交易的手续费,当然用户也可以定义使用其他ERC20代币。
- **社交账户登录和恢复:**为方便开发者打通WEB2和WEB3之间的壁垒,PlatON钱包插件及其SDK集成了社交账户登录和恢复能力,应用链的开发者可以轻松的将社交登录(如Facebook、Google、Apple、Github等)功能内置到dApp中。社交登录既可以方便用户快速登录应用,还可以为WEB3账户绑定一个监护人邮箱。当应用使用合约钱包时,如果用户发生密钥遗失,就可以通过PlatON后台提供的守护邮件域名密钥(Domain Keys Identified Mail)验证服务验证申请重置账户而不至于让用户资产受到损失,进一步增强了用户账户的安全性。

## 4.4 统一的API服务

应用开发者经常要面对一个应用在不同的链上进行迁移和适配的问题,不同的链的各式各样的API接口给开发者造成了很大的适配和调试负担。为了最大程度的给开发者提供便利,PlatON应用链提供了统一的API服务。

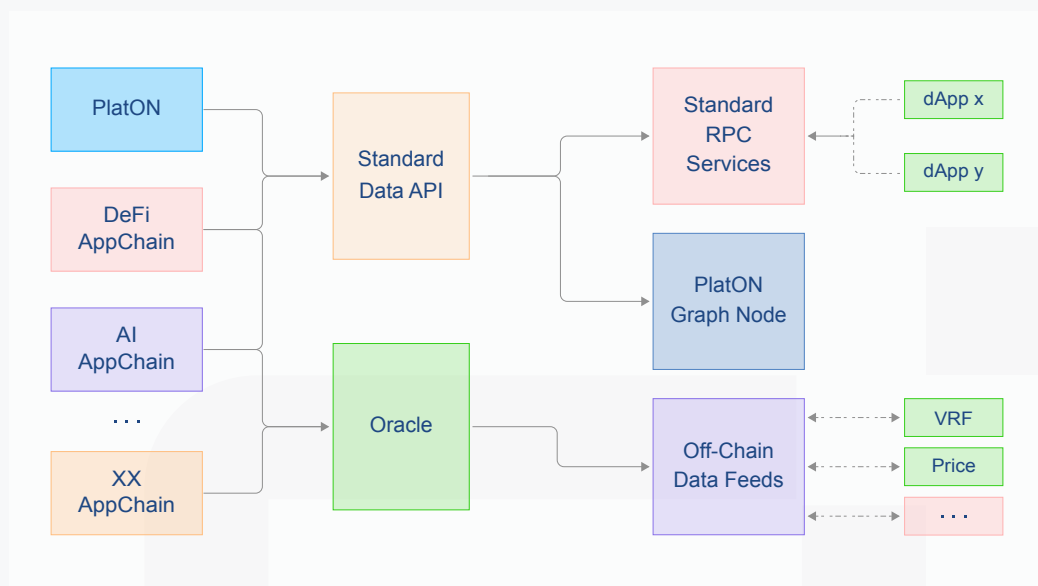


图11 PlatON应用链公共API

### 统一的RPC服务

各个应用链在PlatON的Registry注册成功后,应用链框架将自动根据应用链ID和应用链缺省endpoint通过标准化API接口获取链上数据,并统一转化为以太坊的RPC标准化接口。应用链也可以根据各自的实际情况开发不同的RPC,对于大部分用户来说不需关心不同Appchain之间的差异,只需通过应用链的ID即可轻松使用统一的RPC服务。

### 数据索引服务

应用链注册成功后,应用链框架将随即在PlatON Graph Node中激活该应用链ID,并开始为应用链索引数据,开发者只需要将应用子图部署到PlatON Graph Node,即可轻松获取到用户关心的数据并存入Graph Node。

### 链下数据服务

越来越多的应用需要使用链下数据,通过灵活的链下Data Feeds机制可以让开发者在开发时对链下数据的使用随心所欲而不必担心安全性和实现,PlatON的Oracle预言机服务支持各种常用的链下数据的Feeds,如可验证随机数VRF,Token Price等,除此之外,开发者也可以根据标准接口来定制自己关心的其他链下数据。

## 4.5 隐私计算服务

PlatON的Datum隐私计算平台为数据的隐私保护和数据的资产化提供了一系列方案,实现数据资产发行的高性能web3服务。利用安全多方计算,零知识证明,同态加密,代理重加密等密码学技术对数据进行隐私计算。同时,利用PlatON的区块链基础设施进行数据资产的确权、授权、计算调度、以及数据资产的自动清结算以及监管审计,构建数据、模型和算力的去中心化交易系统。

Datum提供多样化的服务API及SDK,用户可以按需选择相关服务,实现数据传输存托、Data NFT发行、数据资产化管理、数据交易、可信分享、多方数据联合查询计算等需求,提供多样化的隐私增强技术提供数据应用中的全方位隐私保护。使用Datum就能轻松引流数据进入应用链。

Datum对应数据流通的各环节,提供5大类服务能力。

### 数据安全上链服务

以API及SDK形式为数据提供以IPFS、Arweave等去中心化存储以及AWS、Azure、GCP等云存储作为存储介质流转Web3世界,为后续数据资产应用提供基础服务。

### 数据资产化服务

以API及SDK形式提供数据资产发行服务,支持多种NFT合约模板,面向不同应用需求提供快速发布、查看、属性设置服务。

### 数据安全交易服务

以API及SDK形式提供数据资产交易、授权访问、访问鉴权、使用下载、数据一致性校验服务。通过在Data NFT中附加可验证的各类凭证属性,结合代理重加密算法,实现数据访问授权、数据安全分享、所有权转移等功能。

### 数据预言机服务

以API及SDK形式为web2已有的数据服务、数据模型提供web3形态下的链下数据输入到链上合约调用的服务,提供各类服务组件使用户能快速基于数据预言机获取链下数据供链上Dapp使用。

### 数据安全计算服务

以API及SDK形式提供两方、多方数据资产的联合查询分析或计算服务,基于PSI、安全多方计算、同态加密等隐私增加技术提供数据隐私匹配、隐私查询、隐私统计分析及隐私AI能力。





## 第五章/应用场景和案例研究

已经有越来越多的知名应用开启或已准备开始使用应用链承载应用,本节我们将详细讨论最适合构建应用链的领域。

### 5.1 AI大模型应用链

ChatGPT 的横空出世, AI 大模型进入到快速更迭的时代,大模型的应用层面也在持续落地。但大模型生态还处在早期阶段,面临着融资困难、同质化竞争、生产要素缺乏、生态封闭等问题。

PlatON-AppChain 将助力 AI 的发展,构建专用定制化的可控AI应用链,促进大模型的应用落地,建设大模型应用链,创建去中心化的市场来增强AI,实现AI民主。每个人都可访问、拥有大模型,每个开发者甚至用户都应该能够为LLM模型贡献算法和数据,并从模型的未来利润中获得一部分。

- **大模型生态孵化器。**完整的AI产业生态包括、底层基础设施、大模型、提示工程平台和终端应用,大模型AI应用链可以通过Token帮助孵化整个AI产业生态,促进大模型的商业落地。
- **去中心化DAO管理。**当前成功的大模型都是由大型科技公司完成,是封闭源代码且不透明的。通常是由一组封闭的利益相关者管理并决定模型的功能及其开发维护。在大模型应用链中,大模型将完全开放,可以由政府、企业和相关意见领袖/专家组成 DAO 组织,协调模型的开发和维护。平台的通用 Token 用来构建治理框架和投票权,进行相关的经济激励。
- **去中心化GPU计算网络。**人工智能大模型的兴起引发了对 Nvidia A100等高性能显卡的巨大需求,而这些资源集中在少数大公司或云厂商,迫切需要一种经济实惠的按需无服务器计算平台来进行训练工作。基于PlatON应用链,可以构建一个去中心化GPU计算网络。这使得个人和组织可以出租未使用的 GPU 资源,以满足人工智能研究人员和开发人员的需求。

- **去中心化数据标注众包市场。**应用链从 AI数据标注角度出发, 建立一个去中心化的众包平台, 用户可以通过完成数据标注任务获得悬赏。希望通过这种方式, 大幅降低 AI 数据集标注成本, 数据加工者(例如模型数据标注、数据质量评价)也可以通过去中心化数据基础设施参与模型建设并获得对等激励。
- **去中心化 AI Saas 服务。**相较于传统大模型 API需要注册许可。在大模型应用链中, 大模型的 API 是开放的、无需许可的, 大模型的 API 服务可以托管部署在应用链中, 任何人都可以发现、访问和使用。应用链基于去中心化计算网络, 提供大模型的部署托管服务; 大模型在应用链的智能合约中注册登记, 可供付费用户搜索发现调用; 付费用户可对 AI 大模型服务的使用通过 Token 进行支付结算。

## 5.2 GameFi应用链

GameFi游戏正在迈向一个新的时代, 这个领域需要更开放的经济生态和更公平的游戏激励。游戏资产也需要更加透明的平台交易。GameFi经济正在为游戏开发者提供一个新的标准, 来为游戏赋予更多的权力, 围绕着游戏商品来建立经济体系也会将更多的人群带进数字世界中。

越来越多的人开始意识到依托应用链构建链上游戏的重要性, 不仅是因为高性能的应用链会给玩家很好的用户交互体验, 应用链独立的经济体、高可控性以及超低的交易成本也正契合链上游戏的需要。除此之外, 在PlatON-AppChain上构建 GameFi 平台还可从以下两方面给链上游戏应用的发展带来不一样的体验。

- **跨网络游戏市场。**游戏开发者和玩家希望游戏能在廉价且快速的网络上运行, 但也能够在高度流通的网络上来销售商品。依托于 PlatON-Bridge, 游戏开发者可以将某个单一平台的游戏, 转换成全平台的游戏, 用户可以在任意网络中, 用自己的钱包参与到游戏中, 同时用户可以对游戏中的虚拟商品进行跨网络的交易, 提高商品的流通性, 增强可玩性。
- **游戏开发套件。**对于开放者来说, 从头开始构建游戏并不是一件容易的事。PlatON-AppChain为用户提供了开发套件, 具有低延时、高性能的 AppChain节点, 开发者可在应用链上根据游戏的不同组件进行针对性开发, 升级个别组件, 不需要对整个游戏进行更

新, 让游戏在开发和部署上有更好的可组合性。在开销方面, 链上储存的费用降低, 可以让用户节省很高的交互费用。跨平台钱包可以为各类用户提供游戏入口, 与 DeFi生态无缝结合, 无需担心用户流量问题。统一的开发者面板, 可以为开发者获得详细的用户及游戏分析数据, 以及支付系统。

## 5.3 DeFi应用链

随着DeFi项目的蓬勃发展, 每个 DeFi 协议都想寻求扩展, DeFi 协议走向 AppChain 也将是一种必然的趋势。首先, AppChain 可以为 DeFi 带来主权力量, DeFi协议可以通过 AppChain 达到去中心化, 同时摆脱 L1 的运营能力的差别, 避免 L1 影响DeFi业务;其次, AppChain 可以为互操作性提供更多可能。

PlatON- AppChain 利用 PlatON-Bridge 为DeFi 协议的扩展提供帮助, 在链与链之间直接构建资金流动, 有效的保证交付, 能够使 DeFi 得到更广泛应用。最重要的一点, PlatON-AppChain 提供多种去中心共识协议, 避免由中心化的协议 (如中心化排序器) 导致监管方将其贴上证券标签协议, 给DeFi项目提供更多庇护。

- **RWA应用。**通过将有形或无形资产转换为数字代币, 再将其所有权等价值映射到区块链上进行交易。可以达到将现实世界中的资产引入到 DeFi 中并带来更多流动性的目的。RWA 现实资产规模远超加密原生产资产, 通过PlatON-AppChain构建可定制化的RWA应用链, 可以将全球债券、地产、黄金等市场的资产流动性引入到DeFi, 无疑会大幅提升DeFi市场规模。
- **DEX应用。**相对于需要KYC认证的中心化交易所, 自由的DEX (Decentralized Exchange) 交易所更加符合去中心化理念, 这也是其备受追捧的主要原因。PlatON-AppChain可以从三个方面为Dex带来新价值空间:
  - 1)PlatON-AppChain的去中心化属性可以根除做市商的道德风险。
  - 2)开源的代码和协议利于监管审查。
  - 3)应用链上支持各种复杂交易方式包括高频交易, 极大降低交易成本。

## 5.4 DePIN应用链

由于其巨大的资金需求和后勤服务的挑战,传统的电信网络、云服务、移动网络和电网等有形基础设施的部署和管理一直由大型企业主导。这些公司在定价、规则和服务等方面几乎形成了对最终用户的垄断,这导致了行业中缺乏竞争和创新机制,直到区块链和 Web3 出现。

人们希望将现实世界设备引入到物联网(IoT)中,称之为 MachineFi。随着 Token 激励作用在这些现实世界资产(RWA)的合理配置和流通越来越凸显的关键作用,业界将代币激励的实体基础设施网络 TIPIN (Token Incentivized Physical Infrastructure Networks) 和物理工作量证明 PoPW (Proof of Physical Work) 技术结合到一起,称之为去中心化物理基础设施网络 DePIN (Decentralized Physical Infrastructure Networks) DePIN 是一种利用区块链网络结合代币激励产生价值的物理基础设施网络。它代表了区块链技术的新前沿,承载了人们将 RWA 映射到 WEB3 中的愿望,被称为区块链上最真实的应用。DePIN 可以在促进现实世界资源更公平、高效的分配上起到关键作用。

利用 PlatON-AppChain 网络构建去中心化硬件资源市场,可以通过经济激励手段来吸引更多可用的硬件基础设施资源到 WEB3 网络中,利用 PoPW 技术可以将诸多链下资产如存储、传感器、集成电路和数据等有效的映射到链上并提供服务,形成一个物理资产的去中心化分销网络。利用 PlatON-Bridge 可以让这些物理资源和数据进行跨网络流动,为各个项目提供优质硬件资源和数据的同时也增加用户利益。这将有效的促进如算力、存储和数据服务在网络中的分配和分工,为人们提供了一种构建和运营现实世界基础设施的新方式。这种方式更加公平、高效并符合网络参与者的利益,必将孵化出更多优质产品。

## 第六章/应用链的生态系统发展路线图

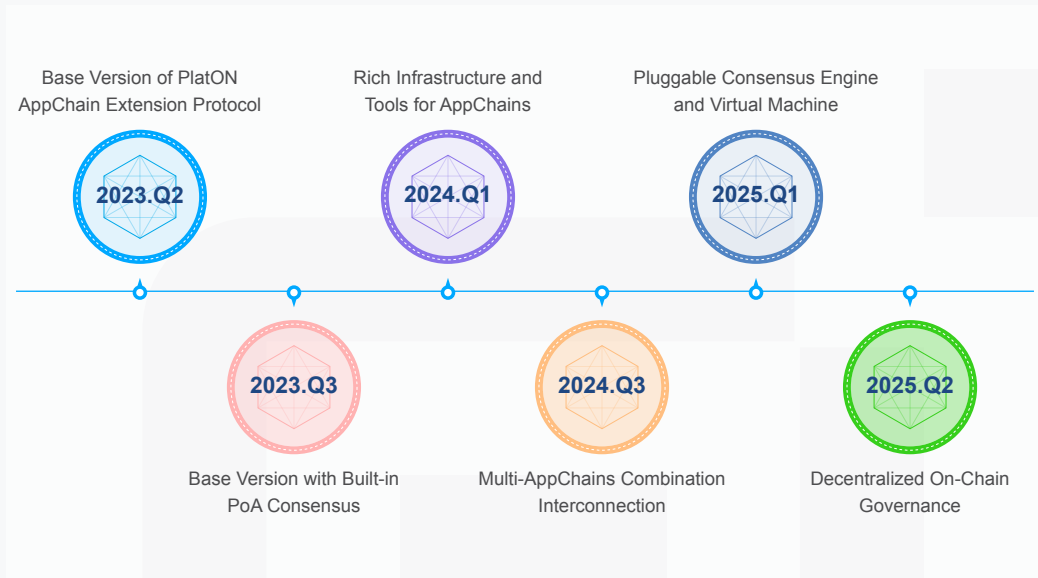


图12 PlatON应用链发展路线

### 2023.Q2

基础应用链扩展协议已经完成,包括应用链治理、节点Staking,以及Checkpoint机制;应用链底层包括Giskard共识、EVM虚拟机、经济模型、链上治理,以及配套基础浏览器、SDK等也已经完成,并已经运行一个应用链测试网络。

### 2023.Q3

内置实现适合大多数应用场景的权威证明共识 PoA机制。提供进一步的配套设施功能,包括完整的钱包ATON、浏览器以及开发工具集 SDK。应用链可通过现有的资产跨链桥跟主链及其他应用链进行互通。

### 2024.Q1

实现更多的配套基础设施,包括统一RPC 服务、数据索引服务、Oracle服务、钱包基础服务等。

## 2024.Q3

PlatON-Bridge 实现消息跨链桥,届时所有PlatON上的应用链可以直接从业务层面管理和配置应用的链间任意消息的跨链规则,实现多链互联互通。

## 2025.Q1

支持可插拔式共识机制和虚拟机,除支持开发者通过标准的共识协议接口和VM接口开发更符合应用本身的共识和虚拟机外,还将提供基于Giskard的优化共识机制和WASM虚拟机供开发者选择。

## 2025.Q2

实现可自定义的链上治理功能,该功能将为应用链灵活的自定义治理提供强有力的协议层保障。